This section is intended to evaluate the quality of, and to determine the degree of compliance to, the standards and procedures applicable to the institution's systems development and programming (S&P) activities. The complexity of the S&P area could range from no in-house programming to complete systems development. The examiner should document any findings, especially those that do not satisfy the recommendations outlined in the 1996 *FFIEC IS Examination Handbook.*

Tier I

PROJECT MANAGEMENT AND CONTROL

1. Obtain applicable committee, management, and users' group minutes, and other written memoranda and instructions that govern the systems and programming function.

   Evaluate the supervision and project control procedures for management to maximize production and resource efficiency and identify and minimize risks in systems development and programming activities. Determine if the control mechanisms used by management are adequate by the review of :

   a. Automated project planning, monitoring, and production software aids used to help control and facilitate the systems and program development process.

   b. Project management reports that set forth the project goals and the current status of major projects, including the programming backlog.

   c. Cost/benefit analysis performed on all major systems development and maintenance projects.

   d. Information systems steering committee minutes or appropriate user committee involvement in setting project priorities and approval review of the development activities.

   e. Any other control mechanisms used by management.

STANDARDS

3. Obtain the "Systems and Programming Standards Manual", memorandum, and other written documentation that govern the activities of the systems and programming function, and:

    a. Determine whether the following written policies, procedures, and standards are adequate:

        (1) Application systems development.
        (2) Application program development.
        (3) Operating system maintenance.
        (4) Program change control.
        (5) Testing.
        (Program and system documentation.
        (7) Implementation.
        (8) Database management systems.
        (9) Backup and recovery.
        (10) Security controls.
        (11) Vendor software support.
        (12) Updating standards and procedures.

APPLICATION SYSTEMS DEVELOPMENT

4. Obtain or prepare a list of all automated applications currently in use or under development. Indicate if the applications were purchased or developed in-house. Also, indicate the person responsible for providing the maintenance support, and determine whether: (For IN-HOUSE developed systems, obtain and review documents generated from the system development process for a selected application system. Trace the documentation from the initial request through the post implementation review.

    a. All required documentation is present and sufficiently detailed to evidence complete compliance with established standards.

    b. The structure of the SDLC planning includes all appropriate phases and whether they were completed as prescribed by the plan.

c. The audit trails, exception reports, and system security designs are adequate.

d. The testing is adequate.

e. The adequacy of user manuals, terminal operating guides, and computer operator instructions.

f. The board, senior management, applicable committees, computer operations, user departments, and audit were involved in all phases of the development process and if such participation was consistent with the plan's review and approval requirements.

g. Based upon documentation, audit reports, committee minutes, memorandum and discussions, the project was successful in meeting the objectives established in the system's definition phase.

APPLICATION PROGRAM DEVELOPMENT

4. Review selected documentation for at least one in-house developed program. Trace the programs' development from the initial request through the post implementation review process, and determine:

   a. If all required documentation is present and sufficiently detailed to evidence full compliance with established programming standards.

   b. The applicability and adequacy of involvement by senior management, committees, computer operations, users, and audits.

   c. Whether the program meets the objectives of the original request, based test results and user feedback.

   For MIS initiated program requests:

   d. Whether standard program request procedures were followed.

   e. If a user department was affected, whether there was appropriate consultation between users and IS departments.

f. Whether appropriate documentation and training was provided to users and computer operations.

OPERATING SYSTEM MAINTENANCE

5. Obtain and review the operating system installation plan, the system generation report, the system log, and other system related activity reports, and determine if: (Review changes made to the operating systems and supporting system software to determine compliance with standards, including adequate internal controls.)

   a. All functional system options are consistent with the approved installation plan.

   b. The overall supervision by management over system programmer activities is adequate.

   c. Supervisory personnel have sufficient technical background to supervise system programmers' activity effectively.

   d. The adequacy of controls over:

      (1) New system installation.

      (2) Implementation of new releases.

      (3) In-house enhancements or tailoring.

      (4) Emergency fixes and other temporary modifications.

      (5) Documentation of changes.

      (6) System testing.

      (7) Management or supervisory approvals.

   e. Controls over data altering utilities, user exits, privileged instructions, and libraries are adequate.

   f. System logs and reports record adequately system programmer activity.

   g. Vendor technicians and outside consultants are subject to the same policies and controls as in-house staff.

PROGRAM MAINTENANCE

6. Review program changes for selected applications to determine compliance with standards and the adequacy of internal control, and determine:

    a. If the program change control procedures provide adequate guidelines to control the function.

    b. If change standards and procedures are adhered to.

    c. If documentation is complete and contains adequate explanations for the omission of any procedures required by the written standards.

    d. The adequacy of involvement of users, audit, and information systems management in the request and approval processes.

    For emergency program fixes and other temporary changes, determine if:

    e. Prescribed procedures are followed.

    f. Documentation is sufficiently detailed to explain the nature of the emergency change, the immediate action taken to address the problem, and subsequent actions to permanently correct the problem.

    g. Emergency changes are incorporated into the next production version of the program.

TESTING

7. Determine whether standards require that:

    a. Test plans explain the overall testing approach and expected results.

    b. The approach includes testing for illogical conditions, out of sequence data, and excess volume.

    c. The scope included all functions, programs, and interface systems, and all test discrepancies are adequately documented and resolved.

d. Users and audit participate in the development of test data and the actual testing phase.

e. All test plans and results are documented and retained.

Based on systems and application program reviews determine if:

f. All testing standards were adhered to.

g. Test documentation is sufficiently comprehensive to support test conclusions.

DOCUMENTATION

8. For the applications selected, determine if:

   a. Overall systems and program documentation adheres to standards.

   b. Documentation is complete and current.

   c. Adequate controls have been established to safeguard documentation.

IMPLEMENTATION

9. Review documentation generated from the implementation process and determine if:

   a. Controls ensure complete integrity of programs between the test and the production environments.

   b. Adequate supervisory review and approval precedes all implementation of program products.

   c. System level implementations are subject to the same controls as application level activity.

DATABASE MANAGEMENT SYSTEMS (DBMS)

10. For the application selected, obtain and review the relevant data base(s) documentation. Review the applicable authorization table to determine who is authorized to update or

otherwise alter indexes, tables, rows, and columns, and determine:

a. The adequacy of written standards and procedures govern all aspects of the function.

b. A database system administrator exists, who has overall responsibility for software installation, software maintenance, performance monitoring, administration of security, database design, and application development.

c. The DBMS function is separate from the systems and programming and operations functions.

d. Controls for changes to the data dictionary.

e. There is a separation of duties within the DBMS function which prevents one individual from controlling the entire operation.

f. Adequate security controls to govern the granting of access rights.

g. Adequate procedures covering database failure, emergency fixes, backup and disaster recovery.

h. The adequacy of controls over access to and usage of query languages and sensitive DBMS utilities.

SECURITY CONTROLS

11. Obtain copies of the security access and control files for the operating system, major third party systems products, and interactive programming facilities. Also, obtain a list of data altering utilities, user exits, user interface programs, and privileged commands. Using these documents determine:

    a. Whether the data security administration function is independent of systems and programming or if sufficient compensating

controls preclude absolute control over major aspects of the function by one person.

b. If all programmers have unique user-IDs and passwords.

c. If auto sign-ons are prohibited.

d. If management has identified and documented all privileged or sensitive programs and library products and if access is on an absolute need basis only.

e. If strict controls govern their use, development, and implementation, including supervisor approval, activity logging, and review procedures.

f. If details of all in-house and vendor exits, and programs designed to run in supervisor state or otherwise capable of by-passing security are provided to the system security administrator and the audit department.

g. If system access and levels of authority are consistent with the job functions.

h. Whether the authority granted under global security systems (RACF, ACF2, TOP SECRET, etc.) do not circumvent local interactive program facility controls.

i. If all changes to the system security software are approved by the system security administrator or advised thereof, and if details of the changes are provided to the audit department.

j. If interactive programming and security software provides an adequate audit trail to identify the programmer, the programs or utilities used, the files or programs accessed, and the nature of the access (change, delete, view, etc.).

k. The adequacy of segregation of duties for application programming, systems programming, computer operation, and system security functions.

l. If management periodically reviews the user authorization file for accounts with unnecessary privileges and whether the review is documented.

m. If physical or logical separation between the production and test environments are maintained.

n. Whether one programmer can develop an entire application system, or independently access, modify, and introduce a program into production.

o. The adequacy of controls over dial-up access.

BACKUP AND RECOVERY

12. Review disaster recovery plans, emergency procedures and other relevant documentation, to determine if: (Coordinate this work with examiner assigned to review Corporate Contingency Planning.)

    a. There are persons with sufficient training and experience to provide backup for the major systems and programming functions.

    b. Operations has a list of person to notify if an application requires immediate maintenance.

    c. Sufficient backup is maintained, including original programs, to ensure continued production should problems be encountered during the maintenance process.

    d. Detailed disaster recovery procedures have been developed and incorporated into the overall disaster recovery plan.

    e. Duplicates of the operating system are available both on and offsite.

    f. Duplicates of the productions programs are available both on and offsite.

    g. All program and system software changes are included in the backup.

h. Duplicates of interactive programming software and other documentation are needed to reestablish both the systems and the application programming functions available offsite.

VENDOR SOFTWARE/SUPPORT

13. Obtain and review copies of all vendor and consultant contracts and agreements, available financial statements, escrow agreements, and applicable written standards, and decide whether:

    a. Software purchase and selection standards require:

        (1) Clear definition of user requirements.

        (2) Clear definition of system requirements (equipment, interface, etc.).

        (3) Cost/benefit analysis.

        (4) Software support (in-house or vendor provided).

        (5) Financial condition of vendor.

        (6) Escrow agreements.

        (7) User documentation and training.

    b. The financial strength and technical expertise of the vendor give assurances that it is capable of providing adequate maintenance support to satisfy the current and future needs of financial institution customers..

    c. The vendor supplies source code or maintains a third party escrow for the benefit of the serviced institutions, and whether the source codes held by the third party are the latest version.

    d. If contract programmers are employed:

        (1) Written contracts are in effect and the adequacy of insurance coverage.

(2) Managements' evaluation of qualifications; the degree of reliance management places on contract programmers; and the level of supervision exercised over the contract programmers adequate.

(3) They are subject to the same policies and procedures as in-house staff.

UPDATING STANDARDS AND PROCEDURES

14. Review the procedures for updating the systems and programming standards manual are decide whether:

    a. Procedures require:

        (1) That one person is responsible for coordinating all updates.

        (2) Updates are appropriately numbered and dated.

        (3) Periodic reviews are conducted to verify older entries.

        (4) Periodic review and approval by management.

    b. Procedures are adhered to.

CONCLUSIONS

15. Review the results of work performed in this section and in sections for Planning, Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

16. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

b. Recommended corrective action for deficiencies cited.

c. Management's proposed actions for correcting deficiencies.

17. Assign a rating. (See Chapter 5 for additional information.)

18. Prepare an index of workpapers for this section of the workprogram.

19. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

20. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

1. Do application system design/development standards require:

   a. An SDLC phase structure that includes:

      (1) User request?

      (2) A feasibility study including cost benefit analysis?

      (3) Detail requirements definitions, based upon user department input?

      (4) General systems design?

      (5) Detail systems design?

      (6) Program development?

      (7) Predetermined progress checkpoints for review?

      (8) Unit testing?

      (9) Systems testing?

      (10) Manual(s) development?

      (11) User training?

      (12) Acceptance testing, with written user approval of the design, test, and final acceptance?

      (13) Conversion?

      (14) Production support?

      (15) Post implementation reviews?

   b. The detail design phase including:

      (1) A system narrative?

      (2) A system flowchart?

      (3) Record layouts?

      (4) Data element definitions?

      (5) Report layouts?

      (6) Screen formats?

      (7) Program specifications?

(8) Test plans?
(9) Project schedules?

c. The project feasibility study provide sufficient detail to justify in-house development of the system as opposed to purchase?

d. A formal request submitted or agreement approved by the head of the user or steering committee before undertaking the project?

e. The definition process include user input at all levels?

f. A statement of purpose and definitions formally presented and approved by the department or committee before actual coding begins?

g. The definition phase including:

(1) All programs or modules of the system and narrative about purpose?

(2) Sample forms and output reports?

(3) Detail security and other features?

h. The presence of all elements of the detail design phase?

i. That elements agree with the definition approved by the user?

j. That all elements been reviewed and approved by appropriate committees?

k. Pre-check intervals that are sufficiently spaced to allow for adjustment to production without disruption to the overall project?

l. Intervals sufficient to allow for a test of key modules?

m. All aspects of the system testing to use live backup data and prepare data designed to exceed acceptable parameters? (Note: Generally, extremely sensitive live data should not be used in the testing process.)

2. Do application programming standards require:

a. Full documentation including:

   (1) program narratives?
   (2) Logic diagrams?
   (3) Input records and descriptions?
   (4) Output record format and descriptions?
   (5) Master file formats and descriptions?
   (6) Source code listings?
   (7) Operating instructions?
   (8) Descriptions of test data?
   (9) User instructions, if applicable?

b. User involvement in major decisions affecting input, logic, flow, and output?

c. Embedded edit routines, including control totals, program edits, and validation checks of inputs before any processing is done?

d. Development of audit trails and exception reports of uncommon transactions?

e. Use of standardized programming languages, naming conventions restart routines, and modular code?

f. Systems programmers to be restricted in their access to application program libraries and documentation?

g. Application programmers be denied access to:

   (1) The computer room?

   (2) Operating system documentation and systems programming work areas?

   (3) Documentation and source codes for programs for which the programmer has no responsibility?

   (4) Documentation and source listings for the operating system?

   (5) Production program libraries?

(6) System level utility programs and other privileged programs and libraries?

(7) Live data files?

h. Procedures to change or remove access for programming personnel that leave the functions?

i. Procedures for terminated or suspected security risk employees?

If automated program development and control software is used:

j. Individual libraries for all programmers?

k. Programmers be restricted to his /her library? If not, is access to other program libraries read only?

l. That programmer sign-ons default to their libraries?

m. That programmers can't escape their libraries into the operating system environment?

3. Do operating systems activity standards include:

a. An overview of the system program function, including responsibilities and prohibited activities?

b. Specific instructions governing each defined task?

c. A detailed description of the operating system including:

(1) Implementation instructions?
(2) Security features?
(3) Description of utilities?
(4) Control or command language requirements?

(5) User error messages?
(6) Error detection and correction features?

(7) List of all files and modules used by the operating system?

d. Standards that require:

(1) Separation of the systems and application programming functions?

(2) Separation of computer operator and system programmer activities?

(3) Separation of the system security and system programming functions?

(4) Complete documentation of the system operating environment, including user enhancements?

(5) Changes to the operating system to adhere to formal change control procedures?

(6) Notification to the security administrator and audit departments of all programs designed to run in supervisor state or otherwise circumvent system security and logging controls prior to implementation?

(7) Identification, documentation, and control of privileged and other sensitive system level programs?

e. Access appropriate for the function performed?

f. Systems programmers be prohibited from accessing the computer's interior or the computer console, except under the supervision of computer operations personnel?

g. That the auditor and security officer maintain a record of all privileged programs, data altering utilities, and other sensitive code?

h. All elements are included in the system generation approved by management?

i. Complete documentation is maintained for all operating systems?

j. A record of all user interfaces, exits, and routines properly documented?

k. Automated logs that produce detailed:

(1) Operating system accesses?
(2) Utility accesses?
(3) Network accesses?
(4) System halts and restarts?
(5) Software modifications?
(6) Accesses to the system clock?

l. That logs be reviewed by supervisory personnel for any unusual activity?

m Whether automated logs can be turned off by unauthorized users?

n. If the logs are retained per a retention schedule?

4. Do program change standards require:

a. Management review to determine feasibility and appropriateness of changes?

b. Testing procedures?

c. User approval prior to implementing changes?

d. Chronology of program changes?

e. Preprinted forms and procedures for requesting program changes, including:

(1) Pre-numbered program change control forms?

(2) A description of the problem or reason for the change?

(3) Approval of the change request by the affected user department?

(4) Names of the programmer making the change?

(5) Signatures of another programmer or supervisor who reviewed and approved the actual program change?

(6) Signatures of the program librarian or quality assurance personnel cataloging the program changes?

(7) Forwarding a copy of the approval to the audit department?

f. Supporting documents, e.g., source listings of codes affected by a change, JCL check listing, and the directory listing of the source and object library?

g. Program modifications be reviewed and approved by the user department prior to implementation?

h. Program documentation be updated to reflect program changes as soon as practical?

i. Temporary program changes be replaced by properly authorized source program changes as soon as practical?

j. Change requests adhere to standards?

k. Change request numbers cross reference all other related documentation?

l. The program modification be tested before installation?

m. Both the program and system documentation be updated to reflect the change?

5. Do documentation standards and procedures require:

a. A formal program documentation librarian function or a person to control documentation?

b. A function independent of other responsibilities that may conflict with documentation control activities?

c. Written policies and procedures governing the function's activities?

d. That documentation librarians' duties include:

(1) Review of documentation during system development to ensure adherence to standards and appropriate authorization of exceptions?

(2) Control and safeguard of documentation?

(3) Revision of documentation to reflect the changes?

(4) Distribution of documentation to authorized parties?

(5) Periodic inventory to account for documentation?

(6) Maintenance of all documentation and standard's manuals to ensure that they are kept current?

(7) Assurance that documentation is adequately backed up offsite.

e. That the librarian control:

(1) All vendor documentation?

(2) All systems documentation?

(3) All application program documentation?

f. That vendors' Technical Engineer's (TEs) documentation is not controlled by the librarian, and that adequate controls have been established to prevent unauthorized access?

g. The librarian function to be available for all shifts? If not, have adequate controls been established for retrieving documentation?

h. That documentation be housed in a physically secure environment?

i. That the environment be protected by fire suppression devices?

6. Do database administration standards require:

a. An administrator to be assigned the responsibility of coordinating and controlling the use of all data bases?

b. The administrator to be independent of the systems programming function?

c. The administrator to establish standards that control overall DBMS activity and include:

   (1) defining the database elements?

   (2) Maintenance of the data dictionary?

   (3) Database design?

   (4) Database operations?

   (5) Security?

d. The administrator's access to live data, application source listings, and other application program documentation be adequately restricted?

e. Subadmistrators to be designated and their authority and activities appropriate and adequately controlled?

f. Access to sensitive DBMS program utilities and high level administrative privileges. Appropriate and regularly monitored?

g. Detailed definitions of data items in a data dictionary or central catalog?

h. That changes to the dictionary be:

   (1) Authorized through the data base administrator?

   (2) Approved by users where applicable?

   (3) Amended in user documentation?

   (4) Adequately tested?

   (5) Reviewed for audit trails and controls?

i. That procedures are in place to ensure that the data dictionary remains current and accurate?

j. The data base administrator have a list of all exit routines that interface the DBMS?

k. The administrator to approve all exits developed in-house?

l. The administrator approve all in-house programs that access the data base?

m. Procedures provide for the prompt notification of users of all changes affecting them?

n. Procedures to cover data base recovery in the event of hardware or software failure?

o. Procedures include periodic dumps of critical data during the processing day?

p. Adequate disaster recovery considerations have been documented and tested?

q. A transaction log provides an audit trail of entries?

r. The log indicates attempts to violate DBMS security?

s. Activity reports and exception reports are reviewed daily?

7. Proceed to procedure 15, Tier I.

Examiner | Date
_____|_____

Reviewer's Initials